UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CITY OF OMAHA POLICE AND
FIREFIGHTERS RETIREMENT SYSTEM,
Individually and on Behalf of All Others
Similarly Situated,

Plaintiff,

vs.

COGNYTE SOFTWARE LTD, ELAD
SHARON and DAVID ABADI

Defendants.

Civil Action No. 1:23-cv-01769

CLASS ACTION

AMENDED COMPLAINT FOR VIOLATION OF THE FEDERAL SECURITIES LAWS

Court-appointed Lead Plaintiff City of Omaha Police and Firefighters Retirement System ("Lead Plaintiff"), individually and on behalf of all others similarly situated, by Lead Plaintiff's undersigned attorneys, alleges the following based upon personal knowledge as to Lead Plaintiff and Lead Plaintiff's own acts; and upon information and belief as to all other matters based on the investigation conducted by and through Lead Plaintiff's attorneys, which included, among other things, a review of the U.S. Securities and Exchange Commission ("SEC") filings by Cognyte Software Ltd ("Cognyte" or the "Company"), press releases and other announcements by the Company, and media and analyst reports about the Company. Lead Plaintiff believes that substantial, additional evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery.

INTRODUCTION

1. This is a securities class action on behalf of all purchasers of Cognyte common stock between February 2, 2021 and January 19, 2023, inclusive (the "Class Period"), against Cognyte and its Chief Executive Officer ("CEO") Elad Sharon for violations of §§10(b) and 20(a) of the Securities Exchange Act of 1934 (the "1934 Act") and Securities and Exchange Commission ("SEC") Rule 10b-5 promulgated thereunder.

2. Cognyte is an Israel-based security analytics software company, which began trading as an independent entity in February 2021 following a spin-off from Verint Systems Inc. ("Verint"). Cognyte's stock trades on the NASDAQ Global Market ("NASDAQ") under the ticker CGNT. According to Cognyte, its software "fuses, analyzes and visualizes disparate data sets at scale to help [its customers] successfully identify, neutralize, and prevent national security, personal safety, business continuity and cyber threats." Its customers include both national, regional, and local governments and governmental agencies, as well as enterprise customers.

3. Because of the industry in which it operates, Cognyte's customer base, business ethics and its compliance with applicable laws, including export control and other laws, enacted to safeguard against misuse of the type of cyber intelligence solutions the Company sold were key areas of investor concern. As an equity research report from William Blair stated:

> "While we believe that there is value to cyber intelligence, we believe that it is important for investors and customers that there are rigid safeguards in place and high transparency to ensure that the software is used in an ethical manner."

4. Throughout the Class Period, Cognyte repeatedly represented that it was operating in an ethical manner, complying with all applicable laws in the jurisdictions in which it operated and did business, and characterized its cyber intelligence solutions as designed to assist government and corporate actors in fending off cyber-attacks, intrusions and other wrongdoing by bad actors. For example, the Company's Code of Conduct, which was referenced in the Registration Statement and posted on Cognyte's website throughout the Class Period, stated that the Company "expect[ed] all of [its] employees and board directors to act ethically and honestly in good faith and to comply with the law," and that "[a]s a global company and good corporate citizen, Cognyte complies with the law in jurisdictions in which [it] operates." In addition, throughout the Class Period, Defendants repeatedly characterized Cognyte's products and software as designed to assist governments, governmental agencies and corporations in "***identify[ing], neutraliz[ing], and prevent[ing] terror, crime, and cyber threats.***" [Emphasis added]

5. These and similar representations made throughout the Class Period were materially false and misleading because Cognyte was not acting in an ethical manner, was not complying with applicable laws, and was not selling its products and software solely to customers interested in neutralizing security threats. Rather, as was later revealed, Cognyte solicited customers and sold its products and services indiscriminately, including reportedly to Myanmar's

dictatorship, and allowed them to be used to target journalists, politicians and other individuals. Among other means, Cognyte used dummy accounts on social media platforms to identify and track targeted individuals around the world and otherwise gathered data on social media platforms in violation of their terms of service.

6. The truth began to come to light on December 16, 2021, when Meta Platforms Inc. ("Meta") issued a Threat Report on the Surveillance-for-Hire Industry (the "Threat Report") after a months-long investigation disclosing that Cognyte was one of seven "cyber mercenary" companies that had indiscriminately targeted journalists, politicians and dissidents using tactics that violated Meta's terms of service contrary to the entities' claims that their "services only target criminals and terrorists." In Cognyte's case, the report stated that Meta had removed approximately 100 accounts on Facebook and Instagram linked to Cognyte and customers of the Company located in 9 separate countries that had been used "to social-engineer people and collect data." In light of its findings, Meta announced that it had banned Cognyte and its customers from its platforms, issued Cease and Desist warnings, "shared [its] findings with security researchers, other platforms and policymakers," and also alerted "people who [it] believed were targeted to help them strengthen the security of their accounts."

7. On this news, the price of Cognyte's common stock fell 5.11%, closing on December 17, 2021, at $18 per share, before declining another 5.5% the next trading day. Cognyte's stock price continued to plummet in the following days, weeks, and months as the Company disclosed that (i) it had to alter its products to comply with Meta's findings, making them less effective and attractive to customers; (ii) revenues and customer counts were declining in the wake of Meta's revelations; (iii) a large investor had informed the Company that it would no longer hold Cognyte stock citing concerns that the Company's indiscriminate sale of its

products and software was contributing to serious human rights violations; and (iv) Cognyte had won a tender to sell intercept spyware to the brutal Myanmar dictatorship in violation of Israeli and other jurisdictions' laws prohibiting the sale of systems of this kind to that country in the wake of the military coup that had seized power. Altogether, Cognyte's stock price has declined from $28 per share on February 2, 2021, the day it began trading following its spin-off from Verint, to $3.57 per share on January 19, 2023, in the wake of the news that it had won the Myanmar tender, a total decline of 87%.

JURISDICTION AND VENUE

8. The claims asserted herein arise under §§10(b) and 20(a) of the Exchange Act (15 U.S.C. §78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. §240.10b-5).

9. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §1331 and §27 of the Exchange Act (15 U.S.C. §78aa).

10. Venue is proper in this judicial District pursuant to §27 of the Exchange Act (15 U.S.C. §78aa). Cognyte common stock is listed on the NASDAQ, which is located in this District, and many of the acts and transactions giving rise to the violations of law complained of occurred here.

11. In connection with the acts alleged in this complaint, Defendants, directly and indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the mails, interstate telephone communications, and the facilities of the national securities markets.

THE PARTIES

12. Lead Plaintiff, City of Omaha, as set forth in its certification (ECF No. 1-1), purchased Cognyte common stock during the Class Period and suffered damages as a result of the federal securities law violations and false and misleading statements alleged herein.

13. Defendant Cognyte is incorporated under the laws of the State of Israel and maintains its principal executive offices at 33 Maskit, Herzliya Pituach, 4673333, Israel. On December 4, 2019, Verint, a New York-based analytics company, announced plans to separate its business into two independent companies: Cognyte Software Ltd., which would consist of Verint's cyber intelligence solutions business, and Verint Systems, Inc., which would consist of Verint's customer engagement business. On February 1, 2021, Cognyte and Verint completed the spin-off and the related separation and distribution. As a result, Cognyte became an independent, publicly traded company with its shares listed on the NASDAQ under the ticker symbol "CGNT." Although it is incorporated in Israel, Cognyte conducts business all over the world through subsidiaries in a host of countries including the U.S.

14. Defendant Elad Sharon ("Sharon") has served as Cognyte's CEO and as a member of Cognyte's Board of Directors (the "Board") since February 1, 2021, the effective date of Cognyte's spin-off from Verint. Previously, Defendant Sharon had served as the President of Verint's cyber intelligence solutions business since February 2016. After joining Verint in 1997, Defendant Sharon held a broad range of management positions in the cyber intelligence solutions business prior to becoming CEO, including Senior Vice President of Products, R&D and Delivery, Senior Vice President of Strategic Programs, and Chief Operating Officer. Throughout the Class Period, Defendant Sharon made statements in the Company's press releases, on earnings conference calls, and during other public events, which, as alleged herein, were materially false

and misleading and violated the federal securities laws. At all relevant times, Defendant Sharon made materially false and misleading statements with scienter.

15. Defendants Cognyte and Sharon are referred to herein as "Defendants."

RELEVANT FACTS

A. Cognyte and Its Business

16. In December 2019, Verint announced its intention to separate its customer engagement and cyber intelligence solutions businesses to create two companies. Cognyte was formed in Israel in the second quarter of 2020 to serve as the holding company of the cyber intelligence business to be contributed by Verint in connection with the spin-off. Cognyte became a standalone public company, independent of Verint, on February 1, 2021, and its common stock began trading on the NASDAQ the following day.

17. Cognyte describes itself as a global leader in security analysis, catering to national, regional, and local governments and governmental agencies, as well as enterprise customers. According to Cognyte, its software is designed to "identify, neutralize, and prevent terror, crime and cyber threats."[1] As of the date of the spin-off, Cognyte had subsidiaries in 13 separate countries including the U.S.

18. Prior to and during the Class Period, Defendants portrayed Cognyte's business as focused on assisting government and corporate security organizations in preventing cyber-attacks, intrusions, and other wrongdoing by bad actors. For example, on January 11, 2021, just weeks before the spin-off, in a discussion at an Analyst/Investor Day event moderated by Matthew H. Frankel, Verint's manager of Investor Relations and Corporate Development, Defendant Sharon and his future colleagues at Cognyte ***touted the capabilities of Cognyte's software as enabling its***

[1] Cognyte Software Ltd. Registration Statement (Form 20-F) (December 22, 2020) at 51.

customers to stay ahead of "criminals, terrorists and hackers all over the world." [Emphasis added.]

19. Similar statements emphasizing the defensive nature of Cognyte's solutions were repeated throughout the Company's presentation and in response to questions from securities analysts. For example, in his prepared remarks, Defendant Sharon stated that ***"[l]eading government and enterprise security organizations around the world partner with Cognyte to address complex security challenges"*** and "rely on [its] security and analytics software every day to generate critical actionable intelligence" without which "they would be flying blind and ***more vulnerable to potential threats***." [Emphasis added.] Likewise during the Q&A portion of the event, Defendant Sharon cited the SolarWinds hack[2] as an example of the type of intrusion that Cognyte's software was designed to prevent:

> [T]he recent cyber-attack on government agencies and commercial organizations, by the way, is a really good example of the challenges and . . . complexity our customers are facing. ***Bad actors today, well-funded organizations with very sophisticated technology. Investigative solutions that Cognyte provides are becoming more important in analyzing cyber-attack vectors, mitigating severe damage***. We believe an open security platform that can fuse very large amounts of data, analyze it and generate real-time intelligence is exactly what our customers need.
>
> ***Usually, after [a] high-profile security event, like SolarWinds, customers all over the world ask themselves if they are ready to deal with such an attack. And when the gaps are identified, they typically allocate budgets and look for modern technology that can help them get ready, and we are well positioned to help them exactly do that.***
>
> [Emphasis added.]

[2] The cybersecurity breach of SolarWinds, a Texas-based network management software company, was one of the most widespread and sophisticated hacking campaigns ever conducted against the federal government and private sector. The Russian Foreign Intelligence Service ("RFIS") injected hidden code into a file that was included in software updates of SolarWinds Orion network management software. This hidden code allowed the RFIS to remotely access infected computer systems.

20. Standalone financial statements for Cognyte included in the January 14, 2021 amended registration statement on Form 20-F (the "Registration Statement") reported revenues of $457 million and $443 million for the pre-spin-off fiscal years ended January 31, 2020 ("FY2019") and 2021 ("FY2020"), respectively.[3] Although Cognyte managed to exceed these totals in its first year as a public company,[4] Cognyte suffered a significant reversal in fortune following the publication of Meta's Threat Report on December 16, 2021. For the year ended January 31, 2023 ("FY2022"), the Company's revenue declined 34% to just $312 million as its customer base dwindled and private sector customers fled.[5] Whereas during the Class Period, Cognyte reported that it had over 1,000 customers, only 400 of which were government entities,[6] by the end of FY2022, Cognyte's customers numbered only in the "hundreds" and were "primarily" in the government sector.[7]

21. As detailed below, Cognyte's diminished revenues and customer base were a direct result of Meta's disclosure in its Threat Report that Cognyte was one of a handful of companies operating on its platforms that had provided intrusive software tools and surveillance services indiscriminately to customers "regardless of who they target or the human rights abuses they might enable."[8] These disclosures contradicted Defendants' consistent portrayal of Cognyte's services as defensive in nature and designed to target criminals and terrorists.

B. Cognyte's Business Is Highly Regulated

[3] Cognyte Software Ltd. Form 20-F at F-23.

[4] Cognyte reported revenues of $474 million for the fiscal year ended January 31, 2022 ("FY2021"). *See* Form 20-F for the fiscal year ended January 31, 2022 ("2021 Form 20-F") at 46.

[5] Form 20-F for the fiscal year ended January 31, 2023 ("2022 Form 20-F") at 33, 47.

[6] Registration Statement at 1, 64; 2021 Form 20-F at 28, 32.

[7] 2022 Form 20-F at 29, 33.

[8] Threat Report at 3. [https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf]

22. Because of the nature of Cognyte's business, the Company is required to abide by a host of laws, rules and regulations. For example, since Cognyte uses social media platforms as a data source, Cognyte is required to abide by the terms of service of those social media platforms. In addition, because Cognyte's products and services are considered defense-related or "dual-use," Cognyte is required to comply with the export control and other laws of Israel governing such products and services, as well as those of any jurisdiction to or from which it exported its products.

1. Cognyte Had to Comply with the Terms of Service of Social Media Platforms

23. Since Cognyte's software operates and collects information on social media platforms, such as Facebook, Instagram, Twitter, Youtube, and VKontakte, Cognyte was required to abide by each platform's terms of service. The terms of service for these platforms generally prohibit the use of bots or other automated means to collect information.

24. For example, Facebook's terms of service provide:

> You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.

Instagram and VKontakte have similar prohibitions.

25. The terms of service of all of these social media platforms also clearly prohibited the use of fake accounts. For example, VKontakte forbids users from "registering as the User on behalf of or instead of another person" or from "misleading other Users as to his/her identity[.]" Likewise, Twitter forbids users from "pos[ing] as someone who doesn't exist to mislead others" about who the user is or who the user represents. Facebook's community standards are even more detailed and specific. Facebook expressly states that it "do[es] not allow people to misrepresent themselves on Facebook, [or] use fake accounts," and warns users not to use Facebook or Instagram to "mislead people or Facebook . . . about [i] the identity, purpose, or origin of the entity

that they represent, . . . [ii] the purpose of an audience or community, . . . [or] [iii] the source or origin of content." Facebook further prohibits users from engaging in the foregoing behaviors on behalf of a foreign or government actor.

26. Violations of the terms of service of any of these social media platforms risked removal of the responsible accounts, especially in cases of repeated or egregious violations, and significant reputational damage in the event the violations became known.

2. Cognyte Had to Comply with Export Control Laws

27. Cognyte and its subsidiaries[9] were required to abide by the export control regulations of any country from which they exported goods and services. Depending on the circumstances, these controls could apply by virtue of the country in which the products were located or by virtue of the origin of the content contained in the products.

28. Since Cognyte is headquartered in Israel, Israel's defense export policy regulated the sale of many of the systems and products the Company developed in Israel. Under Israeli law, a specific export license is required for defense-related hardware, software, services, and know-how exported from Israel unless a license exception or its equivalent was obtained. So-called "dual-use" items that are sold in the commercial market but are used in the defense market as well are also regulated by Israeli law albeit to a lesser extent. Given that most of Cognyte's products were defense-related or dual-use, a license from Israeli authorities was generally required to initiate marketing activities for systems and products the Company sold.

29. Countries in which Cognyte's foreign subsidiaries operated imposed similar controls on some of the Company's systems and products and, like Israel, required Cognyte to

[9] At the time of the spin-off, Cognyte had subsidiaries in Germany, India, Brazil, Canada, Mexico, the United Kingdom, Bulgaria, Taiwan, the Netherlands, Romania, Thailand, Cyprus and the U.S.

obtain specific permits and/or licenses in order to import or export defense-related and "dual-use" systems and products to or from these jurisdictions. For example, under Cypriot law, the export of dual-use items is regulated by the Ministry of Energy, Commerce and Industry, which assesses all export license applications on a case-by-case basis, in compliance with the European Union Global Human Rights Sanctions Regime, as well as the European Union Dual-Use Regulation.

30. Cognyte was also subject to U.S. export control laws administered by the U.S. Commerce Department's Bureau of Industry and Security and the U.S. State Department's Directorate of Defense Trade Controls. Prior to and during the Class Period, these agencies were particularly concerned with controlling the dissemination of cyber surveillance technologies to malicious actors. Indeed, in November 2021, the U.S. Department of Commerce added four surveillance development companies, including Israel's NSO Group and Candiru, to the Entity List[10] based on evidence that they developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. In announcing the Department's decision, the Secretary of Commerce, Gina Raimondo, released a statement stating that the U.S. was "committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organizations here and abroad." Subsequently, in December 2021, the governments of the United States, Australia, Denmark, and Norway, among

[10] The Entity List is made up of entities that the U.S. government has found there is reasonable cause to believe have been involved in, are involved in, or pose a significant risk of being or becoming involved in activities that are contrary to the national security or foreign policy interests of the U.S. government, and those acting on behalf of such entities.

others, pledged to create guidelines to prevent the spread of technologies used to enable human rights abuses.

31. Cognyte was also subject to targeted restrictions imposed by jurisdictions in which it operates or conducts business on business and activities in certain countries and with certain persons, including the economic sanctions regulations administered by the U.S. Treasury Department's Office of Foreign Assets Control. These restrictions included sanctions issued by the U.S. on February 11, 2021, in the wake of that country's military coup against numerous individuals and entities leading Myanmar's military and government and operating in its defense sector.

32. Finally, consistent with the foregoing and as explained below, Cognyte portrayed itself as committed to complying with its own Code of Conduct, which explicitly represented that Cognyte "complies with the law in the jurisdictions in which we operate."[11] Cognyte's Code of Conduct has been in force since Cognyte became a standalone public company in February 2021, and was referenced in the Registration Statement.[12] Throughout the Class Period, the Code of Conduct was posted and available on Cognyte's website.

C. Cognyte Was Materially Breaching the Terms of Service of Social Media Platforms and Relevant Law

33. Unbeknownst to investors, throughout the Class Period, Cognyte was materially breaching both the terms of service of the social media platforms which its products accessed and used, as well as the export control and other laws with which it was required to comply. In particular, as the Meta Threat Report and other media outlets revealed, the Company was

[11] Cognyte Code of Conduct at 44. https://www.cognyte.com/wp-content/uploads/2021/02/cognyte-code-of-conduct-final-2021-february-22.pdf

[12] Cognyte Software Ltd. Registration Statement (Form 20-F) (January 31, 2021) at 112.

indiscriminately selling intrusive software tools and surveillance services to customers who used them to target people across the internet, including journalists, politicians, and others, rather than hackers, criminals, and terrorists.

1. Cognyte Was Breaching Social Media Platforms' Terms of Service

34. As explained by Defendant Sharon during the Company's Q4 2021 earnings call, Cognyte's cyber intelligence solutions are "designed with several components at its core," including "data fusion technologies that aggregate and enrich structured data such as [ ] travel history, for example; and unstructured data such as images, video and social media, from different sources."

35. With respect to social media, unbeknownst to investors, Cognyte, through the use of its Web Intelligence product, was breaching the terms of service of social media platforms in several ways.

36. First, Cognyte's software used prohibited web crawlers or "bots" to "scrape" and collect data from social media platforms.[13]

37. Second, Meta's investigation revealed that Cognyte's Web Intelligence product collected information on targets using fake accounts that were used to search and view people's profiles, Facebook friends, and other publicly available information, to join groups and events on Facebook, and to follow or "friend" targets.[14] In addition, Cognyte's software utilized social engineering tactics such as phishing and fictitious personas to establish contact with targets or persons close to them via email, phone calls, text messages, or direct messaging apps on social media in an effort to build trust, solicit information, and trick victims into clicking on links or

[13] *See* n.8, *supra* at 4.

[14] *Id.*

downloading files that would allow their devices to be hacked.[15] As noted above, these activities violated the terms of service of social media platforms that Cognyte's software solutions used and accessed, which prohibited the use of bots to gather data and barred users from using fake accounts to hide their true identities and mislead other users. Further, the targets of this activity identified by Meta – journalists and politicians around the world[16] – strongly suggested that at least some of Cognyte's customers were government entities, which constituted yet another violation of Meta's terms of service, which prohibit the use of fake accounts on behalf of foreign or government actors.

38. The fact that Cognyte's products and software were being sold and used for these types of cyber mercenary activities in violation of the terms of service of social media platforms remained undisclosed to investors until December 16, 2021, when Meta published the Threat Report detailing the findings of a months-long investigation it had conducted. The Threat Report identified Cognyte as one of seven companies indiscriminately providing surveillance-for-hire services to target people across the internet, including journalists, dissidents, critics of authoritarian regimes, families of opposition members and human rights activists, to collect intelligence, manipulate them into revealing information, and compromise their devices and accounts across the internet.[17]

39. As a result of its investigation, Meta identified and removed approximately 100 accounts on Facebook and Instagram which were linked to Cognyte and customers of the Company in Israel, Serbia, Colombia, Kenya, Morocco, Mexico, Jordan, Thailand, and Indonesia, that had

[15] *Id*. at 5.

[16] *Id*. at 8.

[17] *Id*. at 6.

targeted journalists, politicians, and others.[18] In addition, Meta banned Cognyte from using its platforms and issued Cease and Desist warnings to the Company.[19]

2. Cognyte Was Breaching Export Laws

40. Unbeknownst to investors, Cognyte was also providing its surveillance services and products to customers, including governments responsible for human rights abuses, in violation of export control and other laws the Company was bound to follow.

41. One notable example of this behavior involved the apparent sale of intercept spyware to a Myanmar state-owned telecommunications company, Myanmar Posts and Telecommunications ("MPT") in violation of Israeli and other jurisdictions' export control laws, which banned sales of such technology to Myanmar's dictatorship. On January 15, 2023, HAARETZ and the NGO, Justice for Myanmar, disclosed that, one month before the military coup in Myanmar on February 1, 2021, Cognyte "won a tender to provide an advanced cyber-intelligence system to be installed at the heart of the country's telecommunication network – in order to monitor and eavesdrop on users."[20] The purchase order for the intercept technology was issued to Cognyte "by December 30, 2020," with a scheduled target installation completion date of the end of May/early June 2021. Intercept spyware "monitor[s] network activity, doing everything from locating mobile devices to eavesdropping on conversations, hacking into devices, and extracting text and encrypted messages."[21] Israel, the U.S., and the EU, jurisdictions whose

[18] *Id.* at 8.

[19] *Id.* at 6.

[20] Oded Yaron, "Myanmar Acquired Spyware From Israeli Cyber-Intelligence Firm Cognyte, New Docs Reveal," HAARETZ, Jan. 15, 2023.

[21] *Id.*

export laws Cognyte was required to comply with, have banned sales of technologies of this nature to Myanmar due to its human rights violations.[22]

42. In addition to violating the export laws of multiple jurisdictions in which it operated and did business, the foregoing conduct also violated Cognyte's own Code of Conduct which, as detailed below, required Cognyte's employees, including directors and officers, to be aware of, and compliant with, applicable laws in the jurisdictions in which it operated.

DEFENDANTS' MATERIALLY FALSE AND MISLEADING STATEMENTS AND OMISSIONS DURING THE CLASS PERIOD

A. Defendants' Materially False and Misleading Statements in Cognyte's Code of Conduct

43. Defendants issued a Code of Conduct in February 2021 which was applicable to all Cognyte board members and employees, including employees of any subsidiary of Cognyte "no matter where in the world they [were] located."[23] Each year, Cognyte's employees were required to "certify . . . that they ha[d] complied with the Code and that they were not aware of Code violations by others."[24] In a letter to employees included in the Code of Conduct, Defendant Sharon stated that it was the responsibility "of each of us to understand and be familiar with the Cognyte Code of Conduct."[25] The Code of Conduct was available on Cognyte's website throughout the Class Period.

44. Among other things, the Code stated that:

- Cognyte "expect[ed] all of [its] employees and board directors to act ethically and honestly in good faith and to comply with the law . . .;[26]

[22] *Id.*

[23] *See* n.11, *supra* at 5.

[24] *Id.*

[25] *Id.* at 1.

[26] *Id.* at 3.

- "As a global company and good corporate citizen, Cognyte complies with the law in jurisdictions in which [it] operates;"[27]

- "It [was Cognyte's] policy that directors, officers, employees, and others acting on behalf of Cognyte comply with all applicable governmental laws, rules, and regulations that affect [its] business and the performance of their jobs;"[28]

- Cognyte "[understood] that economic sanctions and embargoes [might] restrict [it] from doing business with certain countries and groups throughout the world;"[29]

- Cognyte "[understood] that [its] products [were] subject to certain U.S. and non-U.S. export laws and regulations."[30]

45. The foregoing statements were materially false and misleading because Cognyte was not conducting its business in an ethical manner and was not complying with applicable law. Rather, as revealed in Meta's Threat Report and articles in other media outlets, Cognyte and its customers were violating the terms of service of Facebook, Instagram, Twitter and other social media platforms that the Company's software accessed and operated on as described in ¶¶23-26, 34-40 above, including by using fake accounts to mislead other users as to its or its customers' identities in order to obtain sensitive information from the users and/or target these individuals with malware to enable full-device digital surveillance. In addition, Cognyte was not operating in compliance with the export control and other laws of multiple jurisdictions in which it did business, which prohibited sales of defense-related and dual-use cyber surveillance technologies to nations and actors that used them to violate individual and human rights as described in ¶¶27-32, 40-42 above. Defendants' failure to disclose Cognyte's unethical and unlawful behavior concealed at least two risks that later materialized – first, that as a result of the Company's flouting of their terms of service, Cognyte risked being banned from the social media platforms that were central

[27] *Id*. at 44.
[28] *Id*.
[29] *Id*. at 45.
[30] *Id*.

to its data gathering activities, thereby jeopardizing the quality and usefulness of its products and services and its ability to maintain and grow its customer base and revenues; and second, that its reputation would be severely harmed by the disclosure that it was conducting its business in an unethical and illegal manner, leading to a loss of customers and declining revenue.

46. The alleged misstatements in Cognyte's Code of Conduct were not puffery; they were material statements of present fact concerning Cognyte's compliance with the law, something that was fundamental to the success of Cognyte's business, especially given its status as a public company in a heavily regulated industry involving dangerous technology that could enable human rights abuses if it fell into the wrong hands.

B. Defendants' Materially False and Misleading Amended Registration Statement

47. On January 13, 2021, Cognyte filed the Registration Statement with the SEC, and it was declared effective on January 15, 2021. The Registration Statement contained several materially false and misleading representations about the Company's customer base and solutions.

48. For example, in a letter to Cognyte shareholders included in the Registration Statement, Defendant Sharon characterized Cognyte as "a global leader in security analytics software that ***empowers governments and enterprises with Actionable Intelligence for a safer world***." [Emphasis added.] He further stated that Cognyte "provide[s] [its] customers with a powerful analytics platform with a rich set of analytics engines, artificial intelligence and machine learning models, workflows, data governance, and visualization tools, to accelerate the investigative process and ***to identify, neutralize, and prevent terror, crime, and cyber threats***." [Emphasis added.]

49. In addition, the Registration Statement stated that the security organizations of Cognyte's government and enterprise customers relied on the Company's solutions to "fuse[],

analyze[] and visualize[] disparate data sets at scale ***to . . . find needles in the haystack[,] . . . accelerate security investigations and connect the dots to successfully identify, neutralize, and prevent national security, personal safety, business continuity and cyber threats***."[31] [Emphasis added.]

50. Further emphasizing the defensive nature of Cognyte's products and services, the Registration Statement contained the following descriptions of the "market trends . . . driving demand for [the Company's] security analytics software" and the solutions offered by Cognyte:

> ***Security Threats are Becoming More Difficult to Detect and Mitigate***. ***Governments and enterprise security organizations face a variety of security challenges, including threats from well-organized and well-funded entities. These threats are becoming increasingly more difficult to detect as bad actors take advantage of the latest technologies to avoid detection and mitigation. Rapid threat detection and quick mitigation are critical to security organizations. Advanced security analytics software can help security organizations find the needles in the haystacks to quickly and effectively address highly sophisticated security attacks.*** As a result, market demand for such advanced software is on the rise.
>
> * * *
>
> Our Solutions
>
> ***Government enterprise customers are responsible for addressing a broad range of security challenges such as crime, terror, cyber-attacks, financial crime and other threats.*** They seek analytics software to transform their security operations and drive more strategic outcomes.
>
> ***Our broad security analytics software portfolio is designed to help customers find the needles in the haystacks, accelerate the investigative process, and successfully identify, neutralize, and prevent terror, crime and cyber threats***.
>
> * * *
>
> ***The stakes are high. An inability to conduct effective and timely security investigations can result in attacks that cost lives and cause significant damage and disruption to the public.*** Therefore, case officers, security analysts and investigative teams are constantly looking for solutions that help them shorten the investigative cycle and drive a higher percentage of conclusive outcomes.[32] [Emphasis added.]

[31] Registration Statement at 1, 60.

[32] Registration Statement at 60-61.

51. The foregoing statements in ¶¶47-50 were materially false and misleading because they portrayed Cognyte's customer base as consisting of governments and corporate enterprise customers seeking defensive solutions against cyber-attacks, intrusions and other threats by terrorists and criminals when, in fact, Cognyte indiscriminately sold its products and software in violation of export control and other laws of Israel and other applicable jurisdictions to customers who used them, including in ways that violated the terms of service of social media platforms, to target politicians, journalists and other individuals.

52. The Registration Statement also purported to warn about risks related to "reputational and political factors related to [Cognyte's] business or operations," stating in relevant part:

> ***We <u>may</u> experience negative publicity, reputational harm, or other adverse impacts on our business as a result of offering certain types of solutions or <u>if</u> we sell our solutions to countries or customers that are considered disfavored by the media or by certain political or privacy organizations, even where such activities or transactions are permissible under applicable laws***. The risk of these adverse impacts ***<u>may</u>*** also result in lost business opportunities that impact our results of operations. These risks ***<u>may</u>*** grow as we grow our business and our brand following the spin-off.[33]
>
> [Emphasis added.]

53. The Registration Statement also purported to warn about risks related to compliance with regulatory requirements stating in relevant part:

> Our business and operations are subject to a variety of regulatory requirements in the countries in which we operate or offer our solutions, including among other things, with respect to trade compliance, anti-corruption, information security, data privacy and protection, tax, labor and government contracts. . . . Regulatory requirements in one jurisdiction may make it difficult or impossible to do business in another jurisdiction. We may also be unsuccessful in obtaining permits, licenses or other authorizations required to operate our business, such as for the marketing or sale or import or export of our products and services.

[33] Registration Statement at 31.

> ***While we endeavor to implement policies, procedures, and systems designed to achieve compliance with these regulatory requirements, we cannot assure you that these policies, procedures, or systems will be adequate or that we or our personnel will not violate these policies and procedures or applicable laws and regulations. Violations of these laws or regulations may harm our reputation and deter government agencies and other existing or potential customers or partners from purchasing our solutions. Furthermore, non-compliance with applicable laws or regulations could result in*** fines, damages, criminal sanctions against us, our officers, or our employees, ***restrictions on the conduct of our business, and damage to our reputation***.[34]

[Emphasis added.]

54. Finally, the Registration Statement also purported to warn about the risks of failing to obtain necessary export and license approvals from Israel and other countries stating in relevant part:

> Some of the technologies that we develop, and that we rely upon in our products, are regulated. . . .
>
> ***If we fail to obtain material approvals in the future, or if material approvals previously obtained are revoked or expire and are not renewed due to factors such as changes in political, government policies or imposition of sanctions, or if existing or future approvals are conditioned on requirements or conditions that we are unable to meet or fulfill, then our ability to sell out products and services to customers outside the country in which they are developed and our ability to obtain goods and services essential to our business could be interrupted, resulting in a material adverse effect on our business, revenues, assets, liabilities and results of operations.***[35]

[Emphasis added.]

55. The statements in ¶¶52-54, above, warning of ***potential*** risks to Cognyte's reputation, consequences from the Company's failure to comply with legal and regulatory requirements, and the adverse consequences of failing to obtain required approvals to export its technologies were materially false and misleading because they portrayed these risks as

[34] Registration Statement at 34.

[35] Registration Statement at 34.

hypothetical when, in fact, Cognyte's violation of social media platforms' terms of service and export control and other laws in jurisdictions in which Cognyte did business were ongoing and posed a clear risk of major damage to Cognyte's reputation and business. These statements were particularly misleading when read in the context of Cognyte's other misstatements, including its representations in the Code of Conduct concerning the Company's compliance with the law and its representations in the Registration Statement concerning the nature of the Company's customers. Taken together, Defendants portrayed Cognyte as a Company that was actively seeking to comply with the law and that was selling its service to governments and corporate leaders to address legitimate security risks. As described herein, these representations were materially false and misleading.

C. Defendants' False and Misleading Q4 and FY 2020 Press Release, Annual Report and Earnings Call

56. On April 29, 2021, Cognyte issued a press release announcing its financial results for Q4 and Fiscal Year ended January 31, 2021. The press release touted "momentum from [Cognyte's] Security Analytics Platform," "significant gross margin expansion," and "multiple seven and eight figure orders," and reiterated that "***over 1,000 government and enterprise customers in more than 100 countries rely on [Cognyte's] solutions to accelerate security investigations and connect the dots to successfully identify, neutralize, and prevent national security, personal safety, business continuity and cyber threats***." [Emphasis added.]

57. That same day, the Company held its Q42020 earnings call with analysts. During the call, Defendant Sharon touted Cognyte's "brand reputation" and stated that Cognyte was "well positioned to continue to win large deals from existing and new customers ***based on the strength of our platform and our reputation for delivering value***." [Emphasis added.] In addition,

Defendant Sharon continued to characterize Cognyte's products and software as defensive in nature stating:

> ***In recent years, security challenges become [sic] internally complex. We all read in the newspapers that well-organized and well-funded illegal entities are becoming harder to detect as they take advantage of the latest technologies to hide in the shadows***.

[Emphasis added.]

58. During the call, Defendant Sharon highlighted a $10 million Q42020 order from ***"[a] national security agency that was looking to shorten the time of security investigations***," and stated that Cognyte had been selected by this customer due to the ability of its open analytics platform "***to keep pace with emerging threats***." [Emphasis added.]

59. Also on April 29, 2021, the Company filed with the SEC its Annual Report on Form 20-F for the fiscal year ended January 31, 2021 (the "2020 Form 20-F"), which was signed by Defendant Sharon. In the 2020 20-F, Defendants again emphasized the defensive nature of its software repeating that the Company's solutions "fuse[d], analyze[d] and visualize[d] disparate data sets at scale ***to help security organizations find needles in the haystacks***[,] . . . ***accelerate security investigations and connect the dots to successfully identify, neutralize, and prevent national security, personal safety, business continuity and cyber threats.***"[36] [Emphasis added]

60. In addition, the 2020 Form 20-F repeated many of the same materially false and misleading statements that had appeared in the Registration Statement about the Company's software solutions and the nature of the threats that they were designed to combat. For example, the 2020 Form 20-F stated:

> ***Security Threats are Becoming More Difficult to Detect and Mitigate. Governments and enterprise security organizations face a variety of security challenges, including threats from well-organized and well-funded entities.***

[36] *See* n.1, *supra* at 26.

> ***These threats are becoming increasingly more difficult to detect as bad actors take advantage of the latest technologies to avoid detection and mitigation. Rapid threat detection and quick mitigation are critical to security organizations. Advanced security analytics software can help security organizations find the needles in the haystacks to quickly and effectively address highly sophisticated security attacks. As a result, market demand for such advanced software is on the rise***.
>
> * * *
>
> ***Our Solutions***
>
> ***Government enterprise customers are responsible for addressing a broad range of security challenges such as crime, terror, cyber-attacks, financial crime and other threats. They seek analytics software to transform their security operations and drive more strategic outcomes.***
>
> ***Our broad security analytics software portfolio is designed to help customers find the needles in the haystacks, accelerate the investigative process, and successfully identify, neutralize, and prevent terror, crime and cyber threats.***
>
> * * *
>
> ***The stakes are high. An inability to conduct effective and timely security investigations can result in attacks that cost lives and cause significant damage and disruption to the public. Therefore, case officers, security analysts and investigative teams are constantly looking for solutions that help them shorten the investigative cycle and drive a higher percentage of conclusive outcomes.***[37]
>
> [Emphasis added.]

61. The foregoing statements in ¶¶56-60 were materially false and misleading because they portrayed Cognyte's customer base as consisting of governments and corporate enterprise customers seeking defensive solutions against cyber-attacks, intrusions and other threats by terrorists and criminals when, in fact, Cognyte indiscriminately sold its products and software in violation of export control and other laws of Israel and other applicable jurisdictions to customers

[37] *See* n.1, *supra* at 27-28.

who used them, including in ways that violated the terms of service of social media platforms, to target politicians, journalists and other individuals.

62. Like the Registration Statement, the 2020 Form 20-F also purported to warn about risks related to "reputational and political factors related to [Cognyte's] business or operations," stating in relevant part:

> ***We <u>may</u> experience negative publicity, reputational harm, or other adverse impacts on our business as a result of offering certain types of solutions or <u>if</u> we sell our solutions to countries or customers that are considered disfavored by the media or by certain political or privacy organizations, even where such activities or transactions are permissible under applicable laws***. The risk of these adverse impacts ***<u>may</u>*** also result in lost business opportunities that impact our results of operations. These risks ***<u>may</u>*** grow as we grow our business and our brand following the spin-off.[38] [Emphasis added]

63. The Registration Statement also purported to warn about risks related to compliance with regulatory requirements stating in relevant part:

> Our business and operations are subject to a variety of regulatory requirements in the countries in which we operate or offer our solutions, including among other things, with respect to trade compliance, anti-corruption, information security, data privacy and protection, tax labor and government contracts. . . . Regulatory requirements in one jurisdiction may make it difficult or impossible to do business in another jurisdiction. We may also be unsuccessful in obtaining permits, licenses or other authorizations required to operate our business, such as for the marketing or sale or import or export of our products and services.
>
> ***While <u>we endeavor</u> to implement policies, procedures, and systems designed to achieve compliance with these regulatory requirements, we cannot assure you that these policies, procedures, or systems will be adequate or that we or our personnel will not violate these policies and procedures or applicable laws and regulations. Violations of these laws or regulations <u>may</u> harm our reputation and deter government agencies and other existing or potential customers or partners from purchasing our solutions. Furthermore, non-compliance with applicable laws or regulations <u>could</u> result in*** fines, damages, criminal sanctions against us, our officers, or our employees, ***restrictions on the conduct of our business, and damage to our reputation***.[39]

[38] *See* n.1, *supra* at 7.

[39] *See* n.1, *supra* at 11.

64. Finally, the Registration Statement also purported to warn about the risks of failing to obtain necessary export and license approvals from Israel and other countries stating in relevant part:

> Some of the technologies that we develop, and that we rely upon in our products, are subject to regulation. . . . Due to such regulation, our international sales and marketing, as well as our international procurement of skilled human resources, technology and components, depend largely on export and marketing license approvals from governmental agencies in Israel and in other countries. ***<u>If</u> we fail to obtain material approvals in the future, or if material approvals previously obtained are revoked or expire and are not renewed due to factors such as changes in political, government policies or imposition of sanctions, or if existing or future approvals are conditioned on requirements or conditions that we are unable to meet or fulfill, then our ability to sell out products and services to customers outside the country n which they are developed and our ability to obtain goods and services essential to our business <u>could</u> be interrupted, resulting in a material adverse effect on our business, revenues, assets, liabilities and results of operations.***[40]

65. The statements in ¶¶62-64, above, warning of potential risks to Cognyte's reputation, consequences from the Company's failure to comply with legal and regulatory requirements, and the adverse consequences of failing to obtain required approvals to export its technologies were materially false and misleading because they portrayed these risks as hypothetical when, in fact, Cognyte's violation of social media platforms' terms of service and export control and other laws in jurisdictions in which Cognyte did business were ongoing and posed a clear risk of major damage to Cognyte's reputation and business. These statements were particularly misleading when read in the context of Cognyte's other misstatements, including its representations in the Code of Conduct concerning the Company's compliance with the law and its representations in the Registration Statement concerning the nature of the Company's customers. Taken together, Defendants portrayed Cognyte as a Company that was actively seeking

[40] *See* n.1, *supra* at 3.

to comply with the law and that was only selling its service to governments and corporate leaders to address legitimate security risks. As described herein, these representations were materially false and misleading.

D. Defendants' Materially False and Misleading Q1 2021 Financial Results and Earnings Call

66. On June 22, 2021, Cognyte issued a press release announcing its Q1 2021 financial results, reporting a "strong" first quarter as "a pure play security analytics public company." In commenting on the quarter, the release quoted Defendant Sharon as touting Cognyte's success at securing "multiple seven-digit and eight-digit orders" and represented that Defendants "continue[d] to see strong market demand for security analytics," which he stated left Cognyte "well positioned for a strong quarter and full year." During the Company's Q1 2021 earnings call with analysts held the same day, Defendant Sharon continued to emphasize that Cognyte's software solutions were designed to assist its customers in addressing "security challenges," stating:

> ***Well-organized, well-funded entities are becoming harder to detect as they take advantage of the [latest] technologies to hide in the shadows. At the same time, there is a growing volume and diversity of structured and unstructured data, and data is fragmented and spread across organization silos, making investigations more difficult***. ***Many customers*** recognize that home-grown solutions cannot keep pace with these evolving security challenges and ***have increasing[ly] sought . . . [s]olutions that [fuse] data [at] scale from different sources [and] generate high-quality insights faster to mitigate the [wide] range of security threats before they unfold.***

[Emphasis added.]

67. During the call, Defendant Sharon highlighted as an example of the successful execution of the Company's strategy a $40 million Q12021 order "***from a national law enforcement organization***" ***that had initially deployed Cognyte's platform "in retail analytics for fighting drug trafficking" and was "now expanding [Cognyte's platform] to add [an] additional***

use case for antiterrorism." In addition, Defendant Sharon touted a recent innovation the Company had developed for "***addressing cryptocurrency investigations***," stating:

> ***Cryptocurrencies are being increasingly used for illegal activities, such as money laundering, extortion, drug transactions, terror funding and cyber-crime. Cryptocurrencies can be anonymous and borderless, and it's a challenge to find who is behind those illicit transactions. Investigations with existing technologies [often] reach a dead-end when trying to determine who is responsible.***
>
> ***We are about to launch a new solution to help security organizations conduct investigations involving cryptocurrencies.*** Our solution will be offered on a subscription basis and is designed to identify illicit transactions and suspects and generate optimal intelligence to successfully complete investigations. Blockchain analytics, as a challenge it poses to security organizations, are good examples of why the rapid pace of innovation is required for our customers to stay ahead of the curve. This is also a good example of how customers can easily deploy new solutions from our open analytics platform.
>
> [Emphasis added.]

68. The statements referenced in ¶¶66-67 above were materially false and misleading because they portrayed Cognyte's customer base as consisting of governments and corporate enterprise customers seeking defensive solutions against cyber-attacks, intrusions and other threats by terrorists and criminals when, in fact, Cognyte indiscriminately sold its products and software in violation of export control laws of Israel and other applicable jurisdictions to customers who used them, including in ways that violated the terms of service of social media platforms, to target politicians, journalists and other individuals.

E. Defendants' Materially False and Misleading Q2 2021 Financial Results and Earnings Call

69. On September 20, 2021, Cognyte issued a press release announcing its Q2 2021 financial results. During the Company's earnings call with analysts that same day, Defendant Sharon once again claimed that the Company's strategy was focused on "empower[ing] ***security organizations*** with an open analytics platform to help them address many different security use

cases," and repeated the remarks he had made on the Q1 2021 earnings call regarding the security challenges facing Cognyte's customers. In addition, as in earlier calls, Defendant Sharon touted a few seven and eight figure orders received in Q2 2021 including (i) a $10 million order from "***an existing national law enforcement organization customer" that had initially deployed Cognyte's platform for investigating drug trafficking and was "now expanding [the] platform to investigate human trafficking;"*** and (ii) a $7 million order ***"from an existing homeland security customer that [was] using [the] platform to investigate cross-border smuggling of drugs and weapons."*** [Emphasis added.]

70. In addition, Defendant Sharon also highlighted Cognyte's customers' purported ***"growing interest in cybercrime,"*** stating:

> ***Cybercrime is becoming more frequent and the methods that are being used are becoming more and more sophisticated, making identifying the bad actors much more difficult. Our customer mission is to identify the bad actors and prevent cybercrime activities that can lead to significant economic losses and security breaches.***
> [Emphasis added.]

71. During the Q&A portion of the call, Defendant Sharon commented on Cognyte's new cryptocurrency use innovation that had been discussed during the prior quarter's earnings call stating:

> [W]e discussed cryptocurrency in previous call. ***We discussed that it's becoming very important for our customers to have this use case because illegal transactions are done in the cryptocurrency ecosystem.*** It's another use case. Actually, our growth plan is relying on evolving the platform to support more and more use cases, and cryptocurrency is one of them. . . .
>
> [W]e launched it last quarter. . . . [W]e are running multiple POCs with customers, and the results so far are encouraging.
>
> [Emphasis added.]

72. The statements in ¶¶ 69-71 above were materially false and misleading because they portrayed Cognyte's customer base as consisting of governments and corporate enterprise customers seeking defensive solutions against cyber-attacks, intrusions and other threats by terrorists and criminals when, in fact, Cognyte indiscriminately sold its products and software in violation of export control and other laws of Israel and other applicable jurisdictions to customers who used them, including in ways that violated the terms of service of social media platforms, to target politicians, journalists and other individuals.

THE TRUTH BEGINS TO EMERGE

73. On December 16, 2021, after the market closed, Meta, the parent company of Facebook and Instagram, issued the results of its "months long" investigation into the "surveillance-for-hire industry," revealing for the first time that Cognyte and six private companies had "regularly targeted, without their knowledge, journalists, dissidents, critics of authoritarian regimes, families of opposition, and human rights activists around the world," and collected intelligence on these people by manipulating them to reveal information and/or by compromising their devices and accounts, in violation of Facebook's community standards and Terms of Service.[41] With respect to Cognyte in particular, the Threat Report revealed that Cognyte "sells access to its platform which enables managing fake accounts across social media platforms including Facebook, Instagram, Twitter, YouTube, and VKontakte (VK), and other websites to social-engineer people and collect data."[42] This conduct "violated multiple Community Standards and Terms of Service," and "given the severity of [its] violations," Meta disabled Cognyte's ability to use its platforms (removing about 100 accounts on Facebook and Instagram), shared its findings

[41] *See* n.8, *supra* at 2-8.

[42] *Id*. at 8.

with security researchers, other platforms and policymakers, issued Cease and Desist warnings, and alerted the individuals who were believed to be targeted to help them strengthen the security of their accounts.[43]

74. Cognyte's violation of Meta's terms of service had grave implications for Cognyte's business. The disclosure that Cognyte had used fake accounts and bots on Meta to assist bad actors in surveilling journalists, politicians and other targets revealed that Cognyte was a far riskier investment than the purveyor of defensive cyber security tools and software aimed at hackers, cyber criminals and terrorists that Defendants had portrayed Cognyte to be in their public statements. While Defendant Sharon sought to minimize the significance of the wrongdoing revealed in the Threat Report in remarks at the January 11, 2022 Needham Growth Conference, in a January 14, 2022 report, Needham's analysts stated that they believed without Meta's data, "the use-case has potential for reduced effectiveness and customer appeal."

75. Following release of the Threat Report, the price of Cognyte's common stock fell 5.11%, closing at $18 per share on December 17, 2021, before declining another 5.5% the next trading day.

76. Then, on December 21, 2021, an article in HAARETZ, citing the Threat Report, raised the possibility that Cognyte and companies like it might not survive.[44] On this news, the price of Cognyte's stock fell 7.70%, closing at $15.70 per share on December 21, 2021, before declining another 4.46% the next trading day.

77. In the wake of these disclosures. the United States government reportedly pressured Israel to enforce its export laws and prevent the spread of harmful cyber technologies. Customers

[43] *Id.* at 6-8.

[44] Sagi Cohen, "'Cyber mercenaries': How Israel's spyware industry is getting slammed around the world," HAARETZ, Dec. 21, 2021.

also began to abandon Cognyte as evidenced by the Company's disappointing Q4 2021 financial and operating results and inability to provide guidance. In this regard, on April 5, 2022, Cognyte reported a "several million dollar[] [revenue miss] below the midpoint of [its] guidance" for Q4 2021, and advised that it was "unable to provide FY23 guidance and long-term targets at this time." While Defendants blamed "***supply chain issues, as well as, a lower conversion of [Cognyte's] pipeline***," [Emphasis added] Cognyte's Annual Report on Form 20-F for the period ended January 31, 2022 (the "2021 Form 20-F"), also released that day, revealed that the Company was forced to modify its solutions in response to the Threat Report, stating in relevant part:

> Our solutions capture, fuse and analyze data collected from various sources, including from commercial web sources and social platforms. Such sources and platforms may allege that our solutions and techniques for capturing and collecting data and information from such sources violate their terms of use or other propriety rights of such sources or of their users. In December 2021, Meta Platforms Inc., or Meta, issued a report alleging that certain solutions offered by us that interface with Facebook and Instagram platforms violates their terms of use. Concurrently with the issuance of the foregoing report, Meta announced that it had removed accounts that it claimed were associated with our solutions and requested we cease data collection from its social platforms. ***In response to Meta's allegations, we made modifications to certain features of our solutions, which impacted the manner our customers can use these solutions***. [Emphasis added.]

78. The response from analysts to these disclosures was swift and negative, with many reducing their price targets, including Wedbush, who lowered its price target from $17 to $9 concluding:

> [T]he Cognyte business model is turning into a debacle of [ ] epic proportions for investors that once believed in the story. Since the spin-off from Verint over the past year, the Cognyte story ha[s] been a nightmare for investors as the execution shortfalls, longer sales cycles, and myriad of challenges has created a perfect storm for the Street. Most troubling to us is that CGNT was unable to guide for 1Q23 and 2023, which means to us that management may not have their arms around the sales execution and headwinds in our opinion.

79. The market responded immediately and harshly. Cognyte's stock price plummeted over 31% on unusually high trading volume, closing at $8.03 per share on April 5, 2022, which was down $3.63 per share from its April 4, 2022, close of $11.66 per share.

80. On June 28, 2022, Cognyte released its Q1 2022 financial results, which badly missed analyst estimates across the board. Cognyte's Q1 2022 revenue of $87 million, for example, represented a year-over-year decline of 25%. Analysts were expecting a decline of only 2%. Once again, the Company blamed supply chain issues and slow pipeline conversion for the disappointing results.

81. Analysts, however, attributed Cognyte's poor results to the reputational fallout from the Threat Report and increased scrutiny of its business. For example, William Blair, downgraded Cognyte to "market perform" and concluded that Cognyte's "low pipeline conversion" issues were related to the negative brand impact caused by scrutiny of its actions and those of other cyber surveillance companies, rejecting the Company's many excuses for the sales decline, including purported supply constraints arising from the pandemic:

> ***Cognyte's management attributed its sales decline to supply chain constraints, a low pipeline conversion, and customer budget uncertainty related to the Russian war. In our view, the low pipeline conversion is a symptom of a broader issue. Cognyte's brand has been negatively impacted by increased scrutiny of the cyber intelligence industry and fellow Israel cyber surveillance firm NSO Group. Last fall, the U.S. government blacklisted the NSO Group after a multitude of reports surfaced that its software was being used inappropriately by governments to spy on citizens with dissenting views. While we believe there is value to cyber intelligence, we believe that it is important for investors and customers that there are rigid safeguards in place and high transparency to ensure that the software is used in an ethical manner.*** [Emphasis added.]

82. On this news, Cognyte's shares declined $1.84, or over 28.66%, to close at $4.58 per share.

83. On December 15, 2022, the Executive Board responsible for overseeing the investments of the Norway Government Pension Fund Global announced it was excluding Cognyte from the fund's investment universe ***citing concerns about the company contributing to serious human rights violations***. The decision was based on a recommendation from the Council of Ethics dated June 17, 2022. [Emphasis added.]

84. On this news, Cognyte's shares declined 7.04%, closing at $2.51 per share on December 15, 2022, before falling another 4.38% the next trading day.

85. Finally, between January 15-18, 2023, Myanmar's apparent acquisition of intercept spyware from Cognyte was disclosed and discussed in a report published by NGO Justice for Myanmar, an in-depth expose in HAARETZ, and an article published by Reuters.[45] In response, Cognyte's stock price declined 5.5% to close on January 19, 2023, at $3.57 per share.

ADDITIONAL EVIDENCE OF SCIENTER

86. The unethical and illegal conduct detailed in ¶¶33-42 above, and the alleged material misstatements and omissions set forth in ¶¶43-72 above, occurred at Defendant Sharon's direction and with his knowledge.

87. At all relevant times, Sharon was CEO of Cognyte. Defendant Sharon, because of his position in the Company, possessed the power and authority to control the contents of Cognyte's filings with the SEC, press releases and presentations to securities analysts, and the Company's disclosures to the market. Defendant Sharon was provided with copies of the

[45] *See* "Israeli Surveillance Firm Cognyte's Business in Myanmar Exposed," Justice For Myanmar, Jan. 15, 2023 (available at https://www.justiceformyanmar.org/stories/israeli-surveillance-firm-cognytes-business-in-myanmar-exposed); Oded Yaron, "Myanmar Acquired Spyware From Israeli Cyber-intelligence Firm Cognyte, New Docs Reveal," HAARETZ, Jan. 15, 2023; Fanny Potkin and Poppy McPherson, "Israel's Cognyte Won Tender to sell Intercept Spyware to Muanmar Before Coup," REUTERS, Jan. 18, 2023.

Company's reports and press releases alleged herein to be materially false and misleading prior to or shortly after their issuance and had the ability and opportunity to prevent their issuance or cause them to be corrected. Defendant Sharon also personally made many of the materially false and misleading statements to the market as alleged herein.

88. Defendant Sharon had a deep familiarity with Cognyte's products and software based on his many years of work at Cognyte and in the division of Verint that became Cognyte. Defendant Sharon had served as the President of Verint's cyber intelligence solutions business, the division of Verint that was spun-off to create Cognyte, from February 2016 to the date of the spin-off. Prior to serving as President of Verint's cyber intelligence solutions business, Sharon had held a broad range of management positions in that business, including Senior Vice President of Products, R&D and Delivery, Senior Vice President of Strategic Programs, and Chief Operating Officer.

89. As CEO of Cognyte, Defendant Sharon received direct reports from Sharon Chouli, Cognyte's Head of Customers, Gil Cohen, Cognyte's Head of Product, Amir Barel, Cognyte's Chief Technology Officer, and Marom Menahem, Cognyte's Head of Europe and Africa. Consequently, Defendant Sharon received and/or had access to information about Cognyte's products and solutions, including where those products and solutions were sold, to whom, and how those products and solutions operated.

90. There is a strong inference that Defendant Sharon knew that Cognyte's software was accessing and operating on social media platforms in violation of their terms of service. According to the Meta Threat Report, fake accounts such as those associated with Cognyte and its customers which were used to target journalists, politicians and others, are typically managed by the service provider for its clients.

91. Similarly, there is a strong inference that Defendant Sharon knew that Cognyte was violating the export control and other laws of jurisdictions in which the Company did business 37ncluding by providing intercept spyware to Myanmar. Defendant Sharon's remarks during the Company's quarterly earnings calls frequently touched upon Cognyte's pipeline and contract wins during the quarter demonstrating that Defendant Sharon had access to and reviewed this information. Moreover, there is a strong inference that Defendant Sharon knew that the Myanmar transaction violated the export control and other laws of several jurisdictions in which Cognyte did business because, for example, Defendant Sharon, a Cognyte employee and director, was obligated to comply with Cognyte's Code of Conduct, which required awareness of and compliance with "all applicable governmental laws, rules, and regulations that affect [Cognyte's] business and the performance of [his] job[]."

92. Furthermore, during the Class Period, Defendant Sharon was personally apprised of issues concerning Cognyte's illicit and/or illegal conduct and the potential fallout therefrom. For example, on July 1, 2021, the Council on Ethics sent a letter to Defendant Sharon on behalf of the Norwegian Government Pension Fund Global, a sovereign wealth fund that owned 1.3% of Cognyte's outstanding shares as of February 2, 2021. The Council on Ethics apprised Defendant Sharon that it had learned about "allegations against Verint Systems Inc (Verint) i.e. in Azerbaijan, Bahrain, Indonesia and South Sudan, where the company or its subsidiaries are said to have sold surveillance products and services used to implement repressive government policies targeting minorities, political activists and journalists." In light of the spin-off, the letter asked Defendant Sharon to explain what steps Cognyte had taken to guard against its products' involvement in human rights abuse citing the risk warning in the Registration Statement (see ¶52, *supra*) concerning the potential for reputational harm that could result. Cognyte sent the Council a

response on August 24, 2021, signed by the Company's Vice President of Risk and Compliance, Ariel Sagee. Although the letter stated that Cognyte was unable to respond to the Council's inquiries about specific customers citing "confidentiality obligations," the letter falsely implied that Cognyte was not selling its solutions to countries engaged in human rights abuses stating that Cognyte (i) "recognize[d] its role to respect internationally recognized human rights," (ii) was "committed to complying with all applicable laws, rules, and regulations, and conducting [itself] in accordance with high ethical standards, consistent with the Company's Code of Conduct," (iii) had taken the opportunity since the spin-off to "enhance its compliance organization and guidelines," and (iv) was "address[ing] human rights and other risks through internal vetting processes, policies, training and awareness, contractual undertakings, and an independently operated Ethics Helpline that [was] available to internal and external stakeholders." The facts that the Council was a large shareholder and its letter had been addressed to Defendant Sharon give rise to a strong inference that Defendants Sharon was aware of and approved Cognyte's misleading response to the Council's inquiries.

93. Cognyte's scienter can be imputed from Defendant Sharon's. Cognyte's scienter is also evidenced by the widespread nature of the misconduct alleged herein, all of which contradicted the alleged misstatements alleged herein.

LOSS CAUSATION

94. Defendants' wrongful conduct, as alleged herein, directly and proximately caused the economic losses suffered by Lead Plaintiff and members of the Class. During the Class Period, Lead Plaintiff and Class members purchased Cognyte common stock at artificially inflated prices caused by Defendants' misconduct as alleged herein. The price of Cognyte's common stock declined significantly when the material risks concealed by Defendants materialized and

Defendants' material misstatements and omissions were revealed to the market causing investors' losses.

95. Before the end of the Class Period, on January 19, 2023, investors had been unaware of the following material facts about Cognyte that had been known to Defendants throughout the Class Period:

(a) Cognyte's business was not limited to assisting governments, governmental agencies and corporate enterprises in combatting hacking, cyber-crimes and terrorists, but also included "surveillance-for-hire" activities on behalf of bad actors that risked enormous reputational and business harm, including lost customers and revenue, if they became known;

(b) Cognyte was violating the terms of service of Facebook, Instagram and other social media platforms by using bots and fake accounts to gather data and/or establish contact with targets or people close to them in an effort to build trust, solicit information, and trick them into clicking on links or downloading files that would allow their devices to be hacked. These activities not only risked serious reputational harm, but also jeopardized both Cognyte's ability to continue accessing and operating on the social media platforms if the violations were discovered, and the effectiveness of its solutions in the event they needed to be modified in order to comply with the social media platforms' terms of service; and

(c) Cognyte was violating the export control and other laws of Israel and other jurisdictions in which it did business, including the U.S., by selling its products and software, many of which were defense-related or "dual-use," to bad actors, including the military dictatorship ruling Myanmar, which used Cognyte's technology to surveil journalists, politicians, and other vulnerable individuals without their knowledge and engage in human rights abuses. These activities risked serious reputational harm if they became known.

96. Defendants' misrepresentations and omissions, as alleged above, misrepresented and concealed the true adverse facts from the market during the Class Period, leading investors to wrongly believe that Cognyte was selling cyber intelligence solutions that were defensive in nature and in an ethical manner that complied with all relevant laws, regulations and the Company's own Code of Conduct.

97. As alleged above, the truth concealed by Defendants' material misrepresentations and omissions was partially revealed to investors for the first time on December 16, 2021, and was not fully revealed until January 19, 2023. For example:

(a) On December 16, 2021, Meta released the Threat Report (i) identifying Cognyte as a "cyber mercenary" engaged in "surveillance-for-hire" activities in ways that violated Meta's terms of service, and (ii) announcing that it had banned the Company from its platforms, issued Cease and Desist letters, and removed approximately 100 fake accounts associated with Cognyte and its customers from its platforms;

(b) On December 21, 2021, media reports issued in the wake of the Threat Report raised the possibility that Cognyte and companies like it might not be able to survive;

(c) On April 5, 2022, Defendants disclosed that Cognyte had missed its revenue guidance for Q42021 due in part to lower conversion of its pipeline and that, in response to the allegations in the Meta Report, it had made modifications to certain features of its solutions, which impacted the manner in which its customers could use them;

(d) On June 28, 2022, Cognyte disclosed financial results for Q12022 that badly missed analyst estimates and again blamed slow pipeline conversion, which analysts surmised was related to the negative brand impact of disclosures that Cognyte's solutions were being used inappropriately by governments to spy on their own citizens;

(e) On December 15, 2022, investors learned for the first time that one of the Company's largest shareholders, the Norway Government Pension Fund Global, after communicating with the Company in July 2021 about possible uses of Cognyte's solutions by countries engaged in human rights abuses, and decided to exclude Cognyte from the fund's investment universe because of its concerns that Cognyte's products and software were contributing to serious human rights violations; and

(f) From January 15-18, 2023, investors learned of Cognyte's apparent sale of intercept spyware to the brutal military dictatorship controlling Myanmar.

98. The damage to Cognyte's reputation and brand from the Meta Threat Report and Meta's decision to ban Cognyte from accessing and using its platforms, Cognyte's poor financial performance following issuance of the Threat Report, the detrimental modifications to the Company's solutions to address Meta's allegations, the decision of Norway's Government Pension Fund Global to exclude Cognyte from the fund's investment universe, and the harm to Cognyte's reputation and brand from the disclosures about its reported sale of intercept spyware to Myanmar were the materialization of the risks concealed by the materially false and misleading representations and omissions detailed above.

99. The market reacted swiftly and negatively to these disclosures as shown in ¶¶73-85 above.

CLASS ACTION ALLEGATIONS

100. Lead Plaintiff brings this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of all purchasers of Cognyte common stock during the Class Period (the "Class"). Excluded from the Class are Defendants and their families.

101. The members of the Class are so numerous that joinder of all members is impracticable. The disposition of their claims in a class action will provide substantial benefits to the parties, Class members and the Court. Cognyte common stock is owned by hundreds, if not thousands, of persons.

102. There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class which predominate over questions which may affect individual Class members include:

(a) Whether the Exchange Act was violated by Defendants;

(b) Whether Defendants omitted and/or misrepresented material facts;

(c) Whether Defendants' statements omitted material facts necessary to make the statements made, in light of the circumstances under which they were made, not misleading;

(d) Whether Defendants knew or deliberately disregarded that their statements were false and misleading;

(e) Whether the prices of Cognyte common stock were artificially inflated; and

(f) The extent of damage sustained by Class members and the appropriate measure of damages.

103. Lead Plaintiff's claims are typical of those of the Class because Lead Plaintiff and the Class sustained damages from Defendants' wrongful conduct.

104. Lead Plaintiff will adequately protect the interests of the Class and has retained counsel who are experienced in class action securities litigation. Lead Plaintiff has no interests which conflict with those of the Class.

105. Class action is superior to other available methods for the fair and efficient adjudication of this controversy.

APPLICABILITY OF THE FRAUD-ON-THE-MARKET PRESUMPTION OF RELIANCE

106. The market for Cognyte common stock was open, well developed, and efficient at all relevant times. As a result of Defendants' materially false and misleading statements and material omissions, the Company's common stock traded at artificially inflated prices during the Class Period. Lead Plaintiff and other members of the Class purchased the Company's common stock, relying on the integrity of the market price of such securities and on publicly available market information relating to Cognyte. Lead Plaintiff and Class members have been damaged thereby.

107. During the Class Period, the artificial inflation of the value of Cognyte common stock was caused by the material misrepresentations and omissions alleged in this Complaint, thereby causing the damages sustained by Lead Plaintiff and other Class members. As alleged herein, during the Class Period, Defendants made, or caused to be made, a series of materially false or misleading statements about the Company's business, prospects, and operations, causing the price of the Company's common stock to be artificially inflated at all relevant times. When the truth was disclosed, it drove down the value of the Company's common stock, causing Lead Plaintiff and other Class members that had purchased the securities at artificially inflated prices to be damaged as a result.

108. At all relevant times, the market for Cognyte common stock was efficient for the following reasons, among others:

(a) Cognyte stock met the requirements for listing and it was listed and actively traded on the NASDAQ, a highly efficient and automated market;

(b) As a regulated issuer, Cognyte filed periodic public reports with the SEC and/or the NASDAQ;

(c) Cognyte regularly communicated with public investors via established market communication mechanisms, including through regular dissemination of press releases on the national circuits of major newswire services and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services; and

(d) Cognyte was followed by securities analysts employed by brokerage firms, who wrote reports about the Company, which reports were distributed to the sales force and certain customers of their respective brokerage firms and were made publicly available.

109. Based on the foregoing, during the Class Period, the market for Cognyte common stock promptly digested information regarding the Company from all publicly available sources and impounded such information into the price of Cognyte stock. Under these circumstances, the market for Cognyte common stock was efficient during the Class Period and, therefore, investors' purchases of Cognyte common stock at artificially inflated market prices give rise to a Class-wide presumption of reliance under the fraud-on-the-market doctrine.

110. In the alternative, Lead Plaintiff and the Class are entitled to a presumption of reliance under *Affiliated Ute Citizens v. United States*, 406 U.S. 128 (1972), because the claims

asserted herein against Defendants are predicated upon omissions of material fact for which there was a duty to disclose.

NO SAFE HARBOR

111. The statutory safe harbor provided for forward-looking statements under certain circumstances does not apply to any of the statements alleged to be false or misleading herein that relate to then-existing facts and conditions, nor does it apply to any material omissions alleged herein. To the extent that statements alleged to be false or misleading are characterized as forward-looking, the statutory safe harbor does not apply to such statements because they were not sufficiently identified as "forward-looking statements" when made, there were no meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the forward-looking statements, and Defendants had actual knowledge that the forward-looking statements were materially false or misleading at the time each such statement was made.

COUNTS

COUNT I
For Violation of §10(b) of the 1934 Act and Rule 10b-5
Against All Defendants

112. Lead Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

113. During the Class Period, Defendants disseminated or approved the materially false and misleading statements specified above, which they knew or recklessly disregarded were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

114. Defendants violated §10(b) of the 1934 Act and Rule 10b-5 in that they:

(a) employed devices, schemes and artifices to defraud;

(b) made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or

(c) engaged in acts, practices and a course of business that operated as a fraud or deceit upon Lead Plaintiff and others similarly situated in connection with their purchases of Cognyte common stock during the Class Period.

115. Lead Plaintiff and the Class have suffered damages in that, in reliance on the integrity of the market, they paid artificially inflated prices for Cognyte common stock. Lead Plaintiff and the Class would not have purchased Cognyte common stock at the prices they paid, or at all, if they had been aware that the market prices had been artificially and falsely inflated by Defendants' materially false and misleading statements and omissions.

COUNT II
For Violation of §20(a) of the 1934 Act
Against Defendant Sharon

116. Lead Plaintiff incorporates and realleges each and every allegation contained above as if fully set forth herein.

117. Defendant Sharon acted as a controlling person of Cognyte within the meaning of §20(a) of the 1934 Act. By reason of his position with the Company, Defendant Sharon had the power and authority to cause Cognyte to engage in the wrongful conduct complained of herein. By reason of such conduct, Defendant Sharon is liable pursuant to §20(a) of the 1934 Act.

PRAYER FOR RELIEF

WHEREFORE, Lead Plaintiff, on Lead Plaintiff's own behalf and on behalf of the Class, prays for relief and judgment as follows:

A. Declaring this action to be a proper class action pursuant to Fed. R. Civ. P. 23, certifying Lead Plaintiff as representative of the Class, and designating Lead Plaintiffs' counsel as Class Counsel;

B. Awarding Lead Plaintiff and the other members of the Class compensatory damages;

C. Awarding Lead Plaintiff and the other members of the Class pre-judgment and post-judgment interest, as well as reasonable attorneys' fees, expert witness fees, and other costs and disbursements; and

D. Awarding Lead Plaintiff and the other members of the Class such other and further relief as the Court may deem just and proper.

JURY DEMAND

Lead Plaintiff demands a trial by jury.

DATED: November 10, 2023

SCOTT+SCOTT ATTORNEYS AT LAW LLP

s/*Deborah Clark-Weintraub*
Deborah Clark-Weintraub
Thomas L. Laughlin, IV
Donald A. Broggi
Claire Sheridan (*Pro Hac Vice Forthcoming*)
Jonathan M. Zimmerman (*Pro Hac Vice Forthcoming*)
The Helmsley Building
230 Park Avenue, 17th Floor
New York, NY 10169

Telephone: 212-233-6444
Facsimile: 212-233-6334
tlaughlin@scott-scott.com
dbroggi@scott-scott.com
csheridan@scott-scott.com
jzimmerman@scott-scott.com

Counsel for Lead Plaintiff City of Omaha Police and Firefighters Retirement System and Lead Counsel for the Class

CERTIFICATE OF SERVICE

I hereby certify that on November 10, 2023, I caused the foregoing to be electronically filed with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the email addresses denoted on the Electronic Mail Notice List.

s/ *Deborah Clark-Weintraub*
Deborah Clark-Weintraub